Journal of Network and Information Security
6 (1), June 2018, 12-17
http://www.publishingindia.com/jnis

Vulnerabilities of Social Networking Sites- An Open Attack Vector for Cyber Criminals

Thilagaraj Ramasubbu[1*] and Deepak Raj Rao G.[2]
[1]Director (Academic) Centre of Excellence in Digital Forensics, & Former Professor and Head, Department of Criminology, University of Madras, Perungudi, Chennai, Tamil Nadu, India. Email: remorems@gmail.com
[2]Assistant Professor (Computer Forensics) LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs, Rohini, Delhi, India. Email: gdeepakrajrao@gmail.com
*Corresponding Author

Abstract: A social networking service is an online service that focuses on facilitating the building of social networks or social relations among people who can share images, activities, backgrounds, or real-life connections. Once information is posted to a social networking site, it is no longer private. The more information shared, the more likely someone could impersonate the user and trick one of their friends into sharing personal information, downloading malware, or providing access to restricted sites. Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation. Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site. Users of online social media become victims for various types of cybercrimes; this may be due to the vulnerabilities present in the application. The advancement in technology provides the social networking sites to be user friendly and quick accessible but there are so many vulnerabilities that can make the users as victim to different types of cybercrimes. This article analysis the various vulnerabilities of social networking sites and how the attackers use this vulnerabilities to take control of the users account and their personal information. Social networking is a magnificent means to hook up with people, create new contacts, share what we familiar with others, and study new things. User must, on the other hand, be conscious of the fact that the web has its own fair share of good and bad components which pulls users to be victim of the vulnerabilities.

Keywords: Malicious website, Privacy issues, Social networking sites, SNS vulnerabilities, Third party application.

I. Introduction

A social networking service is an online service that focuses on facilitating the building of social networks or social relations among people who can share images, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web-based and provide, means for users to interact over the Internet, such as e-mail and instant messaging. Once information is posted to a social networking site, it is no longer private. The more information the user posts, the more vulnerable he or she may become. Even when using high security settings, friends or websites may inadvertently leak your information. Personal information that one shares could be used to conduct attacks against the user or their associates. Due to the various factors, users of online social media become victims for various types of cybercrimes. An empirical study was conducted to find the vulnerabilities of social networking that is used as an attack vector by the cyber criminals.

II. Emerging Trends in social Networking Sites

At the front of evolving trends in social networking sites is the idea of "real-time web" and "location-based." Real-time permit users to put in contents, which is then broadcast as it is being uploaded and this idea is equivalent to live radio and television broadcasts. Twitter set the trend for "real-time" services, in which individuals can broadcast to the world what they are doing, or what is on their minds in an around 140 character limit. Facebook followed soon with their "Live Feed" where individual's actions are streamed immediately as it occurs [1]. At the same time Twitter concentrates on words, Clixtr, one more real-time service, focuses on group picture sharing in which individuals can update their picture streams with pictures while at an occasion. Facebook remains the major picture sharing site. Facebook application and picture aggregator Pixable estimate that Facebook will have 100 billion pictures by summer 2012. In April, 2012, the picture-oriented social medium of network Pinterest had developed into the third biggest social network in the United States.

Social Networking Sites (SNS) like Foursquare obtained fame by permitting the users to "check-in" to location which they are regular at that instant. Gowalla is other such service which works

almost similar manner what Foursquare does, optimizing the GPS in cell phones to design a location-based user experience. Clixtr, even in the real-time space, is also a location-based social networking site, from the time when actions formed by users are mechanically geo-tagged and individual can see actions happening close by throughout the Clixtr iPhone app. Currently, Yelp declared its way into the location-based social networking space from check-ins by means of their cell phone app.

III. Vulnerability of Social Networking Sites

Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation. Information gleaned from social networking sites may be used to design a specific attack that does not come by way of normal usage of social networking site. Some of the vulnerability related to Social Networking Sites are:

A. Social Networking Worms

Social networking worms include Koobface, which has become largest web 2.0 botnet. While a multifaceted threat like Koobface challenges the definition of "worm", it is specifically designed to propagate across social networks, infect more machines into its botnet and hijack more account to send more spam to infect other machines.

B. Phishing Bait

The email that lured you to sign into Facebook, by offering URL called the fbaction.net for the browser. Many Facebook users had their accounts compromised and although it was only a tiny fraction of a percent, when the user realise Facebook has over 350 million users, it's still a significant number [8]. To its credit, Facebook acted quickly, working to blacklist that domain, but lots of copycat efforts ensued. Many social networking sites including Facebook made many efforts to control these sites but similar index page can be easily created to bait the victims to go the malicious sites [12].

C. Data Leaks

Social networks are all about sharing information. Unfortunately, many users share a bit too much about the organisation, project, products, financials, professional, and other sensitive information. Even spouses sometimes over-share top secret project and a few too many of the details associated with the classified information. The resulting issues include the embarrassing, the damaging and the legal.

D. Shortened Links

People use URL shortening services to fit long URLs into tight spaces. They also do a nice job of obfuscating the link so it isn't immediately appear to victims that they are clicking on a malware sites to download and get installed, but not any video. These shortened links are easy to use and ubiquitous. Many of the Twitter clients will automatically shorten any link and others use to see them. This made the user not to avoid the malicious sites by reading its domain name.

E. Advance Persistent Threats (APT)

One of the key elements of advance persistent threats is the gathering of intelligence of persons of interest for which social networks can be a treasure trove of data. Perpetrators use this information to further their threats like placing more intelligence gathering and then gaining access to sensitive systems.

F. Click-jacking

Concealing hyperlinks under lawful clickable comfortable which, when clicked, causes a user to mistakenly perform events, such as downloading malicious code or virus, or sending your ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social networking sites [7].

G. Elicitation

The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. Using elicitation tactics, the attackers do social engineers to obtain personal information through the social media networks.

IV. Other Threats of Social Networking Media

New online social and business networking applications make it increasingly easy for an attacker to explore the trust relationships of a victim by scrutinizing the data that the victim voluntarily, but perhaps unwittingly, provides [3]. For instance, scanning through business networking sites like LinkedIn, or social networking sites like Facebook, My Space, or Friendster, can yield a very complete picture of a person's trust network. By examining the people the victim has linked to via these networking sites the attacker can build a clear picture of the victims trust network.

Once armed with a topology of the victim's trust network the attacker can much more effectively exploit the victim. By identifying trusted third parties and manufacturing or

mimicking relationships with these third parties, the attacker can leverage the trust accorded them, MadIrish.net (2008).

Huber, Kowalski, Nohlberg, & Tjoa (2009), in the article titled Towards Automated Social Engineering Using Social Networking Sites [6] describes how a cleverly written Automated Social Engineering Bot can "learn" a victim's friendship circle and send message automatically in a manner that quite often can pass the Turing test. Into these messages are written malicious code to be loaded into the victim's computer or network. This technique has the advantage of being targeted and automated. The test cited in the abstract showed mixed results in convincing the subjects that the virtual chat was with a real person but concluded that the success rate was good enough to make this approach a cheap and attractive method for a social engineering attack.

The Comsec Consulting report extensively describes the social networking corporate threat, Zalalichin, Efrati, & Cohen (2010). The attack vectors that create a security risk are available mainly due to the ease of social networking media use and the manner in which one can quickly establish trust between an organization's employees and the attacker [10]. In the past, access to valuable company data required the use of bribes, social engineering, and physical entry into a target organization's space. Social networking media allows an attacker, with minimal technical knowledge, the ability to obtain an employee's full name, position, and role within the company, area of specialty, e-mail, and phone numbers, known circle of friends, education, etc. An aggregation of this information allows for a more complete understanding of the target organization, its products, its people, and the critical "inner trust circle", the core decision making group within the organization. Armed with this intelligence, a hostile actor can mount sophisticated social engineering attacks via the internet or other avenues to gain access to the most critical persons and sensitive information with the organization.

McMillan (2011) of Tech Land, the anti-virus firm Sophos discovered that 40% of social network users had encountered malicious attacks [5]. "Despite constant attacks, our data shows that the vast majority of people on Facebook have never experienced a security issue on the site," counters Facebook spokesman Frederic Wolens. Another network security company "Dasient" has proven how easy it is to spread malware through social networks with a recent experiment. Employees of the Dasient, set up accounts at 11 different social networks and posted links to malware sites [11]. Only two networks succeeded in blocking links to sites contained in Google's list of known "poisoned" websites.

In a study conducted to find the vulnerabilities of social networking site across India from the different strata of the users of social networking sites. According to the respondents they use and install third party software available in the social networking sites.

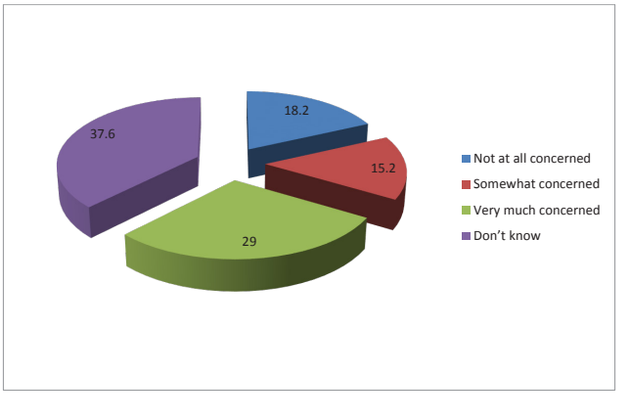

Fig. 1: Vulnerabilities of Third Party Applications in SNS

According to the study, out of 500 respondents, 18.2% of the respondents say they are not at all concerned about it, 15.2% respondents say they are somewhat concerned, 29% respondents say they are very much concerned and rest 37.6% respondents replied that they don't know or not sure about it.

Sites such as Facebook and LinkedIn often allow third-party developers to add their own 'Applications' to the Social Networking Site. These applications often have full access to the user's personal data and profile information. The user is asked to consent to sharing their personal data and often can even choose which specific elements of their data they wish to share. The sad truth is that anyone who is authoring such an application could embed a backdoor that loads JavaScript from a third-party server and eventually leaks all personal data of the SNS user. If the attacker is skilled enough, the application may very well just slip past the Facebook analyst's watchful eyes unnoticed.

Using this vulnerability many companies like Cambridge Analytica use the Facebook users' data to manipulate the perception about the political parties and elections in many countries which includes USA and India.

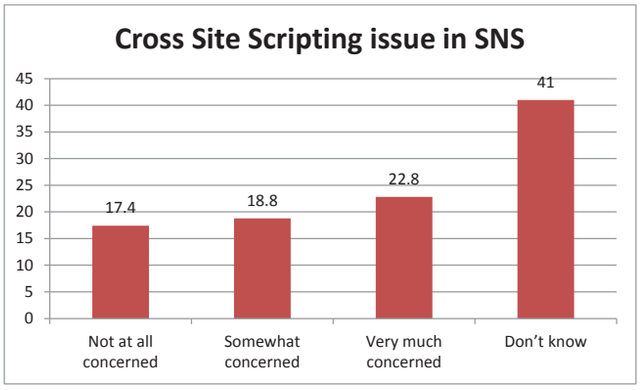

Fig. 2: Cross Site Scripting Issue in SNS

Fig. 2 represents the respondent's opinion about cross site scripting issue in SNS. 17.4% of the respondents say they are

not at all concerned about cross site scripting issue in SNS, 18.8% respondents say they are somewhat concerned about it, 22.8% respondents say they are very much concerned about cross site scripting issue in SNS and rest 41% respondents replied that they don't know or not sure about it.

Timm (2010) XSS is an attack that forces a user's Web browser to execute an attacker's code. The user is the intended victim, and the vulnerable Web site is the conduit for the attack [9]. If an attacker was able to find XSS vulnerability in a popular social networking site, there are so many potential victims are possible which may go to millions. XSS-style attacks have become one of the most predominant attacks using social networking sites.

Samy was the first well-known XSS worm to utilize social networks. The Samy worm spread by exploiting a persistent XSS vulnerability in MySpace.com's personal profile Web page template. At the time of the attack, MySpace was performing some input filtering blacklists to prevent XSS exploits; however, it was early on and they weren't all that good. The author of the worm, Sam Kamkar, was able to successfully bypass the filters and upload his code [10].

It works, when an authenticated MySpace user viewed Samy's profile, the worm payload forced the user's Web browser to add Samy as a friend, add the tag "but most of all, Samy is my hero" to their profile, and alter the user's profile with a copy of the malicious code. The worm started with a single visitor and grew to more than 1,000,000 infected user profiles within the first 24 hours. All it took was for one person to visit Samy, and that person got infected, then everyone that visited the infected person became infected, and so on.

MySpace is not the only site that has encountered these types of attacks, either. Twitter has had numerous XSS attacks, such as Net-Worm.JS.Twettir and StalkDaily, as well as Facebook and Yahoo. We have discussed the ones that have been discovered and we don't know many are there out and which has to be discover yet.

Table I: Links To Malicious Website in SNS

S. No	Links to Malicious websites in SNS	Percent
1	Not at all concerned	18.4
2	Somewhat concerned	17.6
3	Very much concerned	23.2
4	Don't know	40.8
Total		100

Table I represents the respondent's opinion about links to malicious website in SNS. 18.4% of the respondents say they are not at all concerned about links to malicious website in SNS, 17.6% respondents say they are somewhat concerned about it, 23.2% respondents say they are very much concerned about links to malicious website in SNS and rest 40.8% respondents replied that they don't know or not sure about it.

With the openness of social networking sites, the sheer number of users, and the trust that is implied, they have become a haven for the distribution of malware. Malware is a shortened version of the term malicious software, and it is also a very loosely defined term. Infectious malware spreads by replicate itself from one user to the next. Malwares conceal and hides from the user and then steals the user's information the attacker has asked for or does anything else the attacker may want.

According to a Sophos (2010) survey, 40% of social networking users quizzed had been sent malware such as worms via social networking sites, a 90% increase since April 2009; 67% said they had been spammed via social networking sites; and 43% had been on the receiving end of phishing attacks, more than double the figure since April 2009 [5].

In its "Malware Evolution 2008" report, published in February 2009, Kaspersky Lab revealed that malicious code distributed via social networking sites has a success rate of 10 percent in terms of infections, making it 10 times more potent than malware distributed via e-mail.

"In 2008 we increased the collection of malicious files relating to social networks by approximately 26,000," said Tanase (2009), a security researcher for the Kaspersky Lab Global Research and Analysis Team. "In 2008 alone we processed more of those samples than in the total of all years prior to 2008, making the growth rate exponential. Our collection of malicious software samples reached 43,000 at the end of last year."

According to McAfee Report (2009), 800 new variants of the notorious Koobface virus were discovered in March alone. Social networking sites have also been hit by malware hidden in seemingly legitimate third-party applications.

Table II: Crawling Software Used in SNS

S. No	Crawling Software Issue in SNS	Percent
1	Not at all concerned	16.4
2	Somewhat concerned	15.2
3	Very much concerned	20.8
4	Don't know	47.6
Total		100

Table II represents the respondent's opinion about crawling software used in SNS. 16.4% of the respondents say they are not at all concerned about crawling software used in SNS, 15.2% respondents say they are somewhat concerned about it, 20.8% respondents say they are very much concerned about crawling software used in SNS and rest 47.6% respondents replied that they don't know or not sure about it. A crawler is an Internet bot that systematically browses the World Wide Web, typically for the purpose of Web indexing. Using this bot the attacker can search the database of the social networking sites and take all the data that was uploaded by the SNS user, even though they have set all the private policy properly.

In hacking magazine Phrack that described this technique: create malicious URLs for crawlers to follow to conduct attacks that are hard to trace back to the actual attacker. Security researcher Fotonik claims to have reported similar issues to Microsoft and Google. He says that Microsoft made some unspecified changes to its crawler, but that Google did nothing, claiming that its software was working as intended.

V. Privacy issues of Social Networking sites

Privacy concerns with social networking services have increased rising concerns between users on the hazardous of providing more private details and the risk of online predators. Users of the social networking services also need to be conscious of information stealing malwares or viruses. Addition to that, there is an actual confidentiality risk in connection to getting large private details to huge companies or governmental organizations by permitting a profile to be created on a person's performance through which judgment possibly be taken. Moreover, there is matter under the control of data which was changed or deleted by an individual can really be preserved and forwarded to third parties. This risk was focused at the time of the controversial social networking site Quechup gathered e-mail addresses from individual's e-mail accounts for use in a spamming operation.

Cyworld and Facebook's minimum age to become a member is 13 years old, while for MySpace it is 14 years old. Facebook do not permit those 18 years or older to view the profiles of any person under 18, Arrington (2007). However, the Openness Principle is desecrated in regards to minors' being allowed to join sites as their ability to understand privacy policies and terms of use agreements is sternly reduced [2]. If most young people or adults have problem understanding privacy policy information, then minors' will find it extremely difficult to figure out the implications regarding their personal information both what they submit at registration and what they post on their profile page [13].

Confidentiality on social networking sites could be undermined by many aspects. For instance, users can include private details but sites might not get sufficient actions to guard individual's privacy, and third parties recurrently make use of details submitted on social networks for lots of reasons. Many social networking websites provide an API (Application Programming Interface) for third party developers to create applications that can run on its site [14]. These third party applications are very trendy among social network users. Once users add and permit third party applications to access their information, these applications can access user's data automatically. It is also capable of posting on users' space or user's friend's space, or may access other user's information without user's knowledge.

VI. Conclusion and Suggestion

Many people ought to pay the cost once being the prey of cybercrime at diverse social media websites. Many people even cease and disable their social media profile following such awful experiences. It is not the solution to disable or cease the profile when we could diminish the threat of cyber assault on social media accounts by following few simple guidelines.

User must have to decide which data to share and which are not. More or less all social networking websites would provide the choice to determine how much data user wish to share with their pals and other users on that network. User could make their account exceptionally personal or exceedingly public according to their need.If users worried regarding timing when they should set security settings, there is one well-situated online alarm timer that people are making use to attentive themselves at diverse points right through the day that comes in multipurpose in terms of waking up at some stage in vulnerable times of night [15]. This online alarm would ensure user is wake up, and even give them a sensitive means to hear sounds...it is immense for circumstances such as this.

It is suggested to tailor the security setting of user social networking account at the time they are installing their account for the first instance and verify those setting in a daily basis after some time. User should be pretty choosy and vigilant for both send and admit friend request, particularly from unidentified individuals. The user should be very cautious when user are heading for connect any community on those social networking websites. Constantly seek to validate the identity of any person earlier than user heading for send or accept any friend request. User should evade any request from those individual, who are not recognized to them. User should be more cautious if they require giving too much private details at the time of connecting any community.

The FBI's Security Division has issued a draft document to govern the use of social networking media by its employees. This guideline provides background and trend analysis for social networking sites and outlines some general precautions to take while using social networking media, Federal Bureau of Investigation, (2011). This includes prohibiting "accessing publicly accessible social networking sites for non-FBI business proposes from FBI Information Systems" and limiting the amount of personal information that is posted while being alert to social engineering elicitation [4]. In 2011, the FBI added awareness training of social engineering and the threat of nefarious use of social networking media to its annual security training. This was the first time the topics were part of the mandatory training on information security.

It can be concluded that it is possible to reduce the risk of cyber crime through being a little conscious and mindful at the time of using social networking websites. It is necessary to make sure the safety of private information from social networking websites with a small minimal attempt. It is safe not to share password with friends or colleagues or even on any online forum. It is also recommended that not to share details regarding debit or credit card on these social networking websites so as to stay away from credit/debit card scam, too. Social networking is a magnificent means to hook up with people, create new contacts, share what we familiar with others, and study new

things. User must, on the other hand, be conscious of the fact that the web has its own fair share of good and bad components which pulls users to be victim of the vulnerabilities. Hence, it is must for users to watch what they post online and stay safe.

References

[1] C. Fuchs, "*Social media: A critical introduction*," Los Angeles: Sage, 2017.

[2] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11, no. 9, 2006. Available:http://firstmonday.org/issues/issue11_9/barnes/index.html (Accessed May 10, 2013).

[3] D. Boyd, "Why youth love social network sites: The role of networked publics in teenage social life *MacArthur Foundation Series on Digital Learning- Youth, Identity, and Digital Media Volume* (David Buckingham ed.). Cambridge, MA: MIT Press, 2004.

[4] FBI Law Enforcement Bulletin. A Study on Cyber-stalking. Available: http://findarticles.com/p/articles/mi_m2194 /is_3_72/ai_99696472/. (Accessed August 9. 2013).

[5] G. McMillan, "40% of social network users attacked by malware," Available: http://techland.time.com/2011/03/23/40-of-social-network-users-attacked-by-malware/. (Accessed December 19, 2013).

[6] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," Available: http://www.sba-research.org/wp-content/uploads/publications/2009- Huber-Towards Automating Social Engineering Using Social Networking Sites.pdf. (Accessed April 15, 2012).

[7] Mad Irish.net. "Hacking Penetration Testing," Available: http://www.madirish.net/? article=188, (Accessed October 8, 2013).

[8] Symantec, Inc. "Symantec Intenet threat report - volume 16. Symantec.com," Available: http://www. symantec.com/business/threatreport/index.jsp. (Accessed August 4, 2013)

[9] C. Timm, R. Perez, and A. Ely, "Seven deadliest social network attacks," Burlington, MA: Syngress/Elsevier, 2010.

[10] S. Zalalichin, R. Efrati, and T. Cohen, "The social networking corporate threat," Available: http://www.comsecglobal.com/FrameWork/Upload/TheSocialNetworkingCorporateThreatComsec.pdf. (Accessed April 15, 2012).

[11] J. Pomerantz, and F. Stutzman, "Collaborative Reference Work in the Blogosphere," *Reference Services Review*, vol. 34, no. 2, pp. 200-212, 2006.

[12] M. Silic, and A. Back, "The dark side of social networking sites: Understanding phishing risks," *Computers in Human Behavior*, vol. 60, no. C, pp. 35-43, July 2016.

[13] M. Chewae, S. Hayikader, M. H. Hasan, and J. Ibrahim, "How much privacy we still have on social network?" *International Journal of Scientific and Research Publications*, vol. 5, no. 1, pp. 1-5, January, 2015.

[14] Adgaonkar, A. and Shaikh, H. "Privacy in Online Social Networks (OSNs)," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 3, pp. 28-32, March 2015.

[15] P. Tsantarliotis, E. Pitoura, and P. Tsaparas, "Troll vulnerability in online social networks," *The 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM),* pp. 1394-1396, August, 2016.